**IRAN TELECOMMUNICATIONS RESEARCH CENTER (ITRC)**

**Evaluation Technical Report for نرم‌افزار ضد ویروس پاسبان**

Product: نرم‌افزار ضد ویروس پاسبان

Version: 1.0

|  |  |
| --- | --- |
| **Application Number:** | ITRC-AV-2024-001 |
| **Evaluation Level:** | EAL2 |
| **Evaluator:** | ارزیاب سیستم |
| **Company:** | شرکت فناوری پاسبان |
| **Evaluation Period:** | 2025-06-02 to 2025-06-02 |
| **Report Date:** | 2025-06-03 |

# Table of Contents

(Table of contents will be generated automatically)

# Executive Summary

This report presents the results of the Common Criteria evaluation of نرم‌افزار ضد ویروس پاسبان version 1.0 conducted by the Iran Telecommunications Research Center (ITRC).

The evaluation was performed at EAL2 level and covered 5 functional classes. The overall evaluation score achieved was N/A.

# Product Overview

## Product Identification

|  |  |
| --- | --- |
| **Product Name:** | نرم‌افزار ضد ویروس پاسبان |
| **Product Version:** | 1.0 |
| **Developer:** | شرکت فناوری پاسبان |
| **Evaluation Level:** | EAL2 |
| **Application Number:** | ITRC-AV-2024-001 |

## Product Description

نرم‌افزار ضد ویروس پاسبان یک راه‌حل جامع امنیتی برای حفاظت از سیستم‌های پایانی است

## Target of Evaluation (TOE)

محصول نهایی شامل موتور تشخیص، رابط کاربری و سیستم به‌روزرسانی است

# Evaluation Methodology

The evaluation was conducted according to the Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) and the Common Methodology for Information Technology Security Evaluation (ISO/IEC 18045).

## Evaluation Activities

* • Documentation review and analysis
* • Security Target evaluation
* • Functional testing
* • Vulnerability assessment
* • Configuration management review

## Evaluation Period

The evaluation was conducted from June 02, 2025 to June 02, 2025.

# Detailed Evaluation Results

## 1. Malware Detection

|  |  |
| --- | --- |
| **Class Code:** | FAM\_MAL |
| **Subclass:** | Signature-based detection (FAM\_MAL.1) |
| **Status:** | pass |
| **Score:** | N/A |
| **Persian Name:** | تشخیص بدافزار |

### Implementation

پیاده‌سازی تشخیص بر اساس امضا در محصول با استفاده از الگوریتم‌های پیشرفته

### Justification

این کلاس برای حفاظت مؤثر در برابر تهدیدات مرتبط با تشخیص بدافزار ضروری است

### Test Approach

آزمایش تشخیص بر اساس امضا با استفاده از نمونه‌های استاندارد و سناریوهای واقعی

## 2. Malware Detection

|  |  |
| --- | --- |
| **Class Code:** | FAM\_MAL |
| **Subclass:** | Heuristic detection (FAM\_MAL.2) |
| **Status:** | pass |
| **Score:** | N/A |
| **Persian Name:** | تشخیص بدافزار |

### Implementation

پیاده‌سازی تشخیص ابتکاری در محصول با استفاده از الگوریتم‌های پیشرفته

### Justification

این کلاس برای حفاظت مؤثر در برابر تهدیدات مرتبط با تشخیص بدافزار ضروری است

### Test Approach

آزمایش تشخیص ابتکاری با استفاده از نمونه‌های استاندارد و سناریوهای واقعی

## 3. Real-time Protection

|  |  |
| --- | --- |
| **Class Code:** | FAM\_PRT |
| **Subclass:** | File system protection (FAM\_PRT.1) |
| **Status:** | pass |
| **Score:** | N/A |
| **Persian Name:** | حفاظت بلادرنگ |

### Implementation

پیاده‌سازی حفاظت سیستم فایل در محصول با استفاده از الگوریتم‌های پیشرفته

### Justification

این کلاس برای حفاظت مؤثر در برابر تهدیدات مرتبط با حفاظت بلادرنگ ضروری است

### Test Approach

آزمایش حفاظت سیستم فایل با استفاده از نمونه‌های استاندارد و سناریوهای واقعی

## 4. Quarantine Management

|  |  |
| --- | --- |
| **Class Code:** | FAM\_QUA |
| **Subclass:** | File quarantine (FAM\_QUA.1) |
| **Status:** | pass |
| **Score:** | N/A |
| **Persian Name:** | مدیریت قرنطینه |

### Implementation

پیاده‌سازی قرنطینه فایل در محصول با استفاده از الگوریتم‌های پیشرفته

### Justification

این کلاس برای حفاظت مؤثر در برابر تهدیدات مرتبط با مدیریت قرنطینه ضروری است

### Test Approach

آزمایش قرنطینه فایل با استفاده از نمونه‌های استاندارد و سناریوهای واقعی

## 5. Update Mechanism

|  |  |
| --- | --- |
| **Class Code:** | FAM\_UPD |
| **Subclass:** | Automatic updates (FAM\_UPD.1) |
| **Status:** | pass |
| **Score:** | N/A |
| **Persian Name:** | مکانیزم به‌روزرسانی |

### Implementation

پیاده‌سازی به‌روزرسانی خودکار در محصول با استفاده از الگوریتم‌های پیشرفته

### Justification

این کلاس برای حفاظت مؤثر در برابر تهدیدات مرتبط با مکانیزم به‌روزرسانی ضروری است

### Test Approach

آزمایش به‌روزرسانی خودکار با استفاده از نمونه‌های استاندارد و سناریوهای واقعی

# Findings and Recommendations

## Key Findings

ارزیابی 5 کلاس امنیتی انجام شد.

## Recommendations

پیشنهادات بر اساس یافته‌های ارزیابی

# Conclusions

The evaluation is complete. Please refer to the detailed findings for specific conclusions.

# Appendices

## Appendix A: Evaluation Team

Lead Evaluator: ارزیاب سیستم

Email: evaluator@itrc.ir

Organization: ITRC

## Appendix B: References

* • ISO/IEC 15408-1:2009, Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model
* • ISO/IEC 15408-2:2008, Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components
* • ISO/IEC 15408-3:2008, Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components
* • ISO/IEC 18045:2008, Information technology — Security techniques — Methodology for IT security evaluation